A Quantum Safe Mutual Authentication Protocol for Smart Meter Communications with Experimental Evaluation

Rohini Poolat Parameswarath, Chao Wang, and Biplab Sikdar, *Senior Member, IEEE*

***Abstract*—The security landscape will change dramatically with the advent of quantum computers and existing security schemes in various domains including smart grid communications must be updated to make them secure from quantum computer-enabled attacks. In this paper, we propose a quantum-safe mutual authentication protocol, leveraging the concepts of Quantum Key Distribution (QKD) and Quantum Random Number Generator (QRNG), for secure communication between smart meters and a server. Unlike conventional schemes based on cryptographic algorithms that rely on difficulties to solve certain mathematical problems, the proposed protocol is secure against attacks arising from quantum computers. In the proposed protocol, QKD is employed to establish secure keys in smart meter communications with provable security while QRNG provides truly random numbers that are unknown to any eavesdropper. Specifically, we employ the Measurement-Device-Independent Quantum Key Distribution (MDI QKD), a type of QKD whose security does not rely on any assumptions about measurement devices. We provide a formal security proof for the proposed scheme under the real-or-random (RoR) model. Additionally, we conduct a proof-of-concept experimental demonstration, using the secure keys from a MDI QKD system and random numbers from QRNG, to demonstrate the feasibility and practicality of the proposed scheme.**

***Index Terms*—Quantum Key Distribution, Quantum Random Number Generator, security, smart meters.**

I. Introduction

Smart grid networks use advanced technologies to achieve reliable and efficient management and distribution of electricity [1]. The conventional power grid is designed in such a way that the electricity flow is in a unidirectional manner to the customers from the energy supplier. On the other hand, there is a bidirectional flow of electricity and information between the power suppliers and the customers in the smart grid [2]. Smart grids help to improve energy efficiency and maintain the demand-supply balance using mechanisms such as demand-response management [2], [3]. Smart grids also support the adoption of distributed and renewable energy sources into the power grid [4], [5].

Smart meters are key components of the smart grid infrastructure. They monitor the electrical consumption data of consumers and transmit it to a server to make reports on the consumption for services such as electricity billing and demand-side management [6]–[8].

R.P Parameswarath, C. Wang, and B. Sikdar are with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. (Email: rohini.p@nus.edu.sg, wang.chao@nus.edu.sg, bsikdar@nus.edu.sg)

Smart meters handle information about consumers' energy usage patterns, their presence in their residences, individual preferences, and so on [9]. Since smart meters and the server exchange information over the Internet, which is an insecure channel, smart meter communications face several security challenges. As a result, cyber security measures to ensure their smooth operation is an essential requirement in smart meter communications [10].

Several solutions have been proposed to protect smart meter communications from classical cyber-attacks. However, there is a threat arising on the horizon: cyber-attacks enabled by quantum computers. A quantum computer leverages quantum mechanical properties and can perform some calculations exponentially faster than existing computers.

With powerful quantum computers and algorithms, the security of some of the existing advanced metering systems is at stake [11]. As an example, symmetric and asymmetric cryptographic techniques are widely used to build authentication protocols to ensure the security of smart meters. The security offered by asymmetric cryptographic approaches such as Elliptic-Curve Cryptography (ECC) and Rivest–Shamir–Adleman (RSA) comes from the hardness of solving the underlying mathematical problems. For example, the security of RSA is based on the hardness of the prime factorization problem. Shor's quantum algorithm [12] is a quantum cryptanalysis algorithm for factoring that can solve such problems quickly. Grover's quantum search [13] is a key search algorithm that can speed up searches [14]. The security level offered by the symmetric cryptographic key schemes reduces by half when an adversary applies Grover's search [15]. The Advanced Encryption Standard (AES)-128 which has a 128-bit key provides a pre-quantum security of 128 bits but a post-quantum security of only 64 bits [15]. Hence, a workaround to make the symmetric cryptographic schemes resilient to Grover's search is to increase their key sizes. For example, to achieve 128 bits of post-quantum security, AES-256 must be used in contrast to AES-128 which gives 128 bits of pre-quantum security [15]–[17]. AES-256 with a 256-bit key is a recommended symmetric cryptographic scheme for post-quantum security since it provides 128-bits of security against quantum adversaries [16], [18]. However, the key for symmetric encryption is often established between two parties via asymmetric cryptographic techniques, which are vulnerable to attacks from advanced algorithm and hardware developments such as quantum computers.

Thus, the existing security solutions for smart meters can

be weakened by quantum computer-enabled attacks. Hence, any authentication protocol for smart meters should be resilient to future quantum computer-enabled attacks as well, in addition to the classical attacks.

Quantum Key Distribution (QKD) techniques can help to make systems quantum-safe. A QKD scheme helps two entities to establish a common secret key by leveraging the laws of quantum mechanics. A classical communication channel can be passively monitored by an adversary, without the two communicating parties knowing that the messages are being monitored. This is not the case in QKD [19], [20]. Based on the unique properties of quantum mechanics, any eavesdropping on the transmitted quantum states will disturb the quantum system, and will be reflected in the outcome of the system. As a result, legitimate parties can analyse adversary's information on the quantum system and obtain the secure keys that are secure against adversary's side-information. Since its inception, QKD has developed significantly from laboratory demonstrations to the field deployment of networks, using either standard telecommunication optical fibres or free-space as the quantum channel [21]. Therefore, by leveraging the advantages of QKD technology, critical infrastructures such as smart grids can significantly enhance their security against the upcoming threats posed by quantum computers.

In this work, we employ Measurement-Device-Independent Quantum Key Distribution (MDI QKD) [22]–[24] in the proposed protocol. In addition to providing provable security for sharing secret keys among distant parties, MDI QKD offers another advantage that its security does not rely on any assumptions about measurement devices, which are considered the most vulnerable part of practical QKD implementations. Consequently, MDI QKD provides a great balance between practicality and implementation security.

Another critical parameter in cryptographic protocols for critical infrastructures such as smart grids is random numbers. Random numbers provide the unpredictability and uniqueness required in cryptographic protocols to protect against various attacks. For example, in authentication protocols, random numbers ensure that each transaction is unique and help to prevent replay attacks. However, the widely adopted pseudo-random number generators, as their name suggests, are predictable as long as its algorithm and seeds are known [25]. By leveraging intrinsic randomness in quantum physical processes, QRNG protocols can produce certifiable random numbers that are secure against side-information held by potential adversaries.

Thus, the proposed protocol for smart meter communications is secure against future quantum computer-enabled attacks by using secure keys from the QKD and truly random numbers from QRNG.

A. Related Work

Over the last few years, several research results have been published in the literature in the context of smart meter communications. While some papers analyzed the security risks associated with smart metering systems, others have proposed authentication schemes to address these security risks. In this subsection, we discuss some of the recently published authentication schemes for smart meter communications.

A secure scheme to establish a key between smart meters and service providers was proposed in [6]. This scheme is efficient in terms of both communication and computational costs. The authors of [6] also presented a performance analysis using an advanced RISC machine (ARM) chip which demonstrated the protocol's effectiveness. Abbasinezhad-Mood and Nikooghadam [26] presented an elliptic curve cryptography (ECC)-based self-certified scheme to distribute keys among smart meters and service providers to enable secure communications. Since the scheme in [26] is a self-certified scheme, it eliminates the issues associated with certificate management. However, Srinivas et al. [27] reported that the scheme in [26] does not provide strong replay attack protection. Further, they proposed an authenticated key exchange scheme employing the ECC-based Schnorr's signature scheme. Odelu et al. [28] proposed an authenticated key agreement scheme for smart meter communications considering the Canetti–Krawczyk (CK) adversary model. Another key agreement scheme between the smart meter and the service provider based on ECC was proposed in [29]. However, the scheme in [29] does not address privacy concerns in smart meter communications. The authors of [29] reported that the authentication scheme in [28] does not preserve the anonymity of smart meters and involves heavy computational costs by employing the bilinear pairing technique. Another authentication mechanism for smart metering infrastructure employing ECC was proposed in [30]. It is lightweight and provides mutual authentication between the smart meter and the gateway. Gope and Sikdar [31] proposed an authentication protocol to secure smart grid communication. However, their protocol requires Physical Unclonable Functions (PUFs) to be installed in smart meters which are vulnerable to Machine Learning (ML) or modeling attacks [35]. Mahmood et al. proposed an ECC-based authentication and key agreement scheme for smart grid communications in [32]. Abbasinezhad-Mood and Nikooghadam [33] highlighted the limitations of the scheme in [32]. The scheme in [32] is vulnerable under the CK model. It does not protect from session-specific temporary information attacks and does not provide perfect forward secrecy and private key leakage security [33]. Based on these analyses, Abbasinezhad-Mood and Nikooghadam proposed a security-enhanced ECC-based authentication scheme that is secure under the CK attack model in [33]. However, the entities in [33] use the same token for all iterations of the protocol. Hence, two sessions of the same entity can be linked. As a result, the scheme in [33] does not provide unlinkability. Also, Abbasinezhad-Mood and Nikooghadam proposed a password-authenticated key exchange protocol based on extended Chebyshev chaotic maps to read smart meters in [34]. It provides anonymity together with other desired security features to smart meters. We note that the protocols mentioned above have limitations such as being vulnerable to certain attacks or having high computation costs. Another very important factor that the

TABLE I
A BRIEF COMPARISON WITH RELATED SCHEMES

Scheme	Primitives Used	Advantages	Limitations
Abbasinezhad-Mood et al. [6]	ECC, Bilinear map	• Key establishment scheme • Performance analysis using ARM chip	• Does not offer quantum security
Abbasinezhad-Mood and Nikooghadam [26]	ECC	• Self-certified key distribution scheme • Mutual authentication	• Does not offer quantum security
Srinivas et al. [27]	ECC-based Schnorr's signature	• Authenticated key exchange scheme • Mutual authentication	• Does not offer quantum security
Odelu et al. [28]	Bilinear pairing, ECC	• Authenticated key agreement scheme • Mutual authentication	• Does not preserve the anonymity of smart meters • Heavy computational costs • Does not offer quantum security
Wu et al. [29]	ECC	• Secure key agreement scheme • Mutual authentication	• Does not address privacy concerns • Does not offer quantum security
Garg et al. [30]	ECC	• Mutual authentication • Lightweight	• Does not offer quantum security
Gope and Sikdar [31]	PUF	• Authenticated key agreement scheme • Lightweight	• Requires PUFs which are vulnerable to machine learning or modeling attacks • Does not offer quantum security
Mahmood et al. [32]	ECC	• Authentication and key agreement scheme	• Does not provide perfect forward secrecy and private key leakage security • Vulnerable under CK attack model • Does not offer quantum security
Abbasinezhad-Mood and Nikooghadam [33]	ECC	• Authentication scheme • Lightweight • Secure under CK attack model	• Does not provide unlinkability • Does not offer quantum security
Abbasinezhad-Mood and Nikooghadam [34]	Extended Chebyshev chaotic map	• Password-authenticated key exchange protocol	• Does not offer quantum security
Proposed protocol	• QKD • QRNG	• Mutual authentication • Provides quantum security by using QKD to establish a secure key. Since QKD is based on principles of quantum mechanics, an adversary cannot break it even with quantum computing capabilities • QRNG provides secure and true random numbers	• Initial cost of the deployment. With the development of the technology, the cost is expected to go down

above protocols overlooked is the imminent threat of quantum computer-enabled attacks. The existing protocols that employ asymmetric cryptographic methods, such as ECC, to build authentication schemes are vulnerable to quantum computer-enabled attacks since the underlying mathematical problems are not difficult to solve for a quantum adversary. Table I provides a brief comparison of the proposed protocol with related works in terms of features, limitations, and advantages.

There have been certain attempts by researchers to use QKD in various applications. The authors of [36] mentioned that QKD can be applied to the existing optical fiber channels in distributed energy resource (DER) systems, thus leveraging the existing infrastructure. Zefan et al. [37] proposed a real-time QKD-enabled microgrid testbed. Their work shows the feasibility of constructing a QKD system in the microgrid. Kumar et al. [38] proposed an authentication scheme using QKD and classical identity-based authentication. The authors of [39] proposed a quantum encryption scheme for power data transmission leveraging ping-pong QKD protocol. The authors of [40] analyzed the feasibility of using QKD in DER systems in terms of network performance and implementation cost. These works point to the feasibility of using QKD in protocols. Further, we recommend the review papers [20], [21], [41] for additional reading on QKD and the papers [25], [42] for more details on QRNG.

B. Motivation

In addition to resilience against the existing forms of cyber-attacks, smart meter communications should also be resilient to future attacks by an adversary with quantum computing capabilities. Most of the existing protocols in the literature rely on asymmetric cryptographic techniques for mutual authentication and key agreement between the smart meter and server. As the security offered by asymmetric cryptographic techniques relies on the complexity of the underlying mathematical problems, a quantum adversary can break the security offered by such systems. Hence, it is important to design a protocol for smart meter communications whose security does not rely on the complexity of the underlying mathematical problems. QKD, based on the principles of quantum mechanics, helps to establish secure keys while providing provable security even against quantum adversaries. Hence, QKD is an ideal option for establishing secure keys in smart meter communications. Also, the commonly used pseudo-random number generators in existing

protocols are predictable if their algorithm and seeds are known. They can be replaced by QRNGs that can generate secure random numbers. Motivated by these requirements, we propose a mutual authentication protocol to secure smart meter communications leveraging QKD and QRNG.

C. Contributions

The key contributions of this paper are as follows:

- **Design of a quantum-safe mutual authentication protocol for smart meter communications leveraging QKD and QRNG:** We bring together the QKD technique and QRNG together with lightweight operations to build a lightweight and quantum-safe protocol for smart meter communications. In the registration phase, a key is established between the smart meter and the server in a secure manner by using the QKD technique. Before data transfer, the smart meter and the server mutually authenticate using the key established through the QKD process.
- **Protection from conventional and future quantum computer-enabled attacks:** The proposed protocol does not make any assumption on the complexity of underlying mathematical assumptions to achieve security. Rather, it leverages QKD which provides secure keys based on the principles of quantum mechanics. Hence, the proposed protocol offers protection from conventional and future quantum computer-enabled attacks that can weaken the complexity of mathematical assumptions.
- **Privacy of the customers:** The proposed protocol ensures the privacy of the customers. With the proposed protocol, an attacker cannot identify the source of the data. Also, two authentication sessions of the same customer cannot be linked.
- **Security analysis:** We provide a formal security proof and informal security analysis to demonstrate that the proposed protocol offers robust security and ensures privacy of the customers.
- **Experimental analysis:** We also experimentally deploy the MDI QKD system for secure key distribution and QRNG system for random number generation to demonstrate the feasibility of the proposed protocol. In practical QKD implementations, the measurement device is considered the most vulnerable part. In the proposed protocol, we employ MDI QKD whose security does not make any assumptions about measurement devices. Thus, by employing MDI QKD, we achieve both practicality and implementation security.

D. Paper Organization

The rest of this paper is organized as follows. In Section II, we discuss the background knowledge required for the proposed protocol. The system model, adversary model, and security goals of the proposed protocol are presented in Section III. The proposed authentication protocol is presented in Section IV. In Section V, we provide formal and informal security proofs for the proposed protocol. We present experimental details of the protocol implementation with MDI QKD and QRNG systems in Section VI. Section VII presents a performance analysis and we conclude this paper in Section VIII.

II. Preliminaries

In this section, we provide a quick overview of the fundamentals of quantum key distribution and quantum random number generators.

A. Basic Quantum Terminologies

First, for completeness, we provide an overview of some of the basic quantum terminologies relevant to this paper.

Quantum bit (Qubit): Qubit is the basic unit used to encode data in quantum computing. A bit in classical computing can only exist in either a '0' or '1' state. In addition to these two states, qubits can also exist in a superposition to have a linear combination of these states [43].

Entanglement: An important property of qubits is entanglement, where the states of two qubits are correlated, even if they are separated by a long distance. In an entangled state, two members of a pair exist in a single quantum state. When the state of one qubit is changed, the state of the other qubit also will change immediately in a predictable way, despite the distance between them [43].

Quantum channel: A quantum channel is a channel used to transmit quantum information, which is assumed to be accessible by eavesdroppers with unlimited computing resources, and their actions do not violate quantum physics. A quantum channel can be made up of optical fiber or free space.

Bell-states and Bell-state-measurement: Bell-states are four specific states of two qubits. Bell-states are created when the two qubits are maximally entangled [44]. Bell-state-measurement is a joint quantum-mechanical measurement performed on the two qubits to find which of the four Bell states the two qubits are in [44].

B. Quantum Key Distribution

Quantum key distribution is a promising quantum technology that can establish secret keys among distant parties in an untrusted network [20], [41]. The main advantage of QKD is that its security is solely based on the laws of quantum mechanics rather than on computational complexity. For example, randomly prepared quantum states sent to distant parties through an untrusted quantum channel cannot be perfectly known or cloned by any eavesdropper without introducing disturbances to the quantum system. Consequently, QKD can provide secure communication with provable security. This makes it resilient to future hardware or algorithm advancements, and safe against the emerging threats from quantum computers. The MDI QKD is a QKD protocol whose security does not rely on any assumptions about measurement devices [22]–[24]. In MDI QKD, each participant holds a quantum transmitter, randomly prepares

quantum states, and sends them to the untrusted receiver for joint quantum state measurement (Bell-state measurement). This process works as entanglement swapping, making the security analysis of MDI QKD equivalent to the time-reversed version of entanglement-based QKD protocols [45]. In this case, any attacks based on imperfect quantum receivers can be treated as part of the untrusted quantum channel. As a result, MDI QKD is immune to all side-channel attacks on the quantum receiver, which is typically considered the most vulnerable component in practical QKD implementations [23]. Additionally, MDI QKD provides a natural star topology, rendering it ideal for expanding the network. The proposed protocol is built upon secure keys from the MDI QKD protocol [24]. The working flow of a generic MDI QKD protocol is given below [46]:

In a MDI QKD system, each user Alice and Bob holds a quantum transmitter, which can randomly prepare quantum states, and send them to a central untrusted server Charlie for Bell-state measurements. Alice and Bob repeat the following steps until the conditions in the Sifting step are met.

- Quantum state preparation: Alice and Bob prepare a quantum state independently, based on their random choices of systems settings, including intensity selection, basis selection, and a random bit.
- Quantum state distribution: Alice and Bob send their states to Charlie via a quantum channel, which is used for transmitting quantum information. This quantum channel is assumed to be accessible by eavesdroppers with unlimited computing resources, and their actions do not violate quantum physics.
- Quantum state measurement: Charlie performs Bell-state measurements on the received quantum states and announces the measurement results via a public classical channel.
- Sifting: If Charlie announces a successful Bell-state measurement result, Alice and Bob broadcast their intensity and basis settings. They will stop the above quantum state preparation for measurement processes when they have collected a sufficient number of successful measurement events. Next, Bob flips his bits depending on the basis choice and the reported Bell-state.
- Parameter estimation: Alice and Bob select a random subset from the Z-basis random bits and use the X-basis random bits to determine statistical parameters, including counting rate and error rate. If the error rate exceeds a predefined threshold, the protocol is aborted.
- Error correction: Alice and Bob perform information reconciliation to ensure that Bob's raw key matches Alice's. If it fails, the protocol is aborted.
- Privacy amplification: A random universal hash function is used to extract two shorter strings based on the estimated statistical parameters and the upper bound on the eavesdropper's information. The concatenation of these extracted strings forms the final secret keys.

The key rate, l, of MDI QKD protocol is given below [24], [46] :

$$\begin{aligned} l \leq & n_0 + n_1[1 - h(e_1)] - \mathrm{l_{EC}} \\ & - \log \frac{8}{\varepsilon_{\mathrm{corr}}} - 2\log \frac{2}{\varepsilon' \hat{\varepsilon}} - 2\log \frac{1}{2\varepsilon_{\mathrm{PA}}}. \end{aligned} \tag{1}$$

where n_0 is the number of occurrences of events in which one of the participants does not send any photons, n_1 is the number of occurrences of events in which each participant sends one photon, e_1 is the error rate of the one photon events, $h(e_1)$ is the binary entropy of e_1, $\varepsilon_{\mathrm{corr}}$ is the maximum probability that both participants' bit strings are not identical, $\mathrm{l_{EC}}$ is the number of leaked bits from error correction, and ε values are security parameters. For further details on security proof definitions and key rate formula, we refer the readers to [24] and [46].

C. Quantum Random Number Generator

Random numbers are fundamental and critical resources in cryptographic applications. By utilizing inherently random quantum processes, a QRNG can generate true random numbers that are both uniform and unpredictable [25], [42]. One example of QRNG involves measuring a quantum system prepared in a superposition of the measurement basis states. The measurement outputs are inherently random, following Born's rule. Additionally, quantum technologies allow for the generation of certified randomness, ensuring that the outcome is uniformly distributed and independent of side information. For example, device-independent (DI) QRNG exploits the correlations observed when measuring entangled systems and certifies the randomness by the violation of Bell inequality [47], [48]. In this work, we use random numbers produced by an integrable QRNG based on an uncharacterized measurement device with provable security [49].

III. System Model, Adversary Model, and Security Goals

A. System Model

The system model is illustrated in Figure 1. For the efficient management of resources, the proposed scheme considers a decentralized architecture where multiple servers are deployed. Each server is in charge of the smart meters in a particular area. This architecture helps to reduce the latency. We consider a residential area where a smart meter is installed in each house. The smart meters collect and record data such as voltage levels and electric energy consumption of the households, and transmit the collected data to the server in charge of that particular residential area. We denote the smart meters as $\mathcal{SM}_x$ for $x \in \{1, 2, \cdots\}$ and servers as $\mathcal{S}_y$ for $y \in \{1, 2, \cdots\}$. The smart meters and servers are registered with a central untrusted authority $\mathcal{CA}$. The smart meters and servers hold a quantum transmitter each, which can randomly prepare quantum states and send them to $\mathcal{CA}$ for Bell-state measurement.

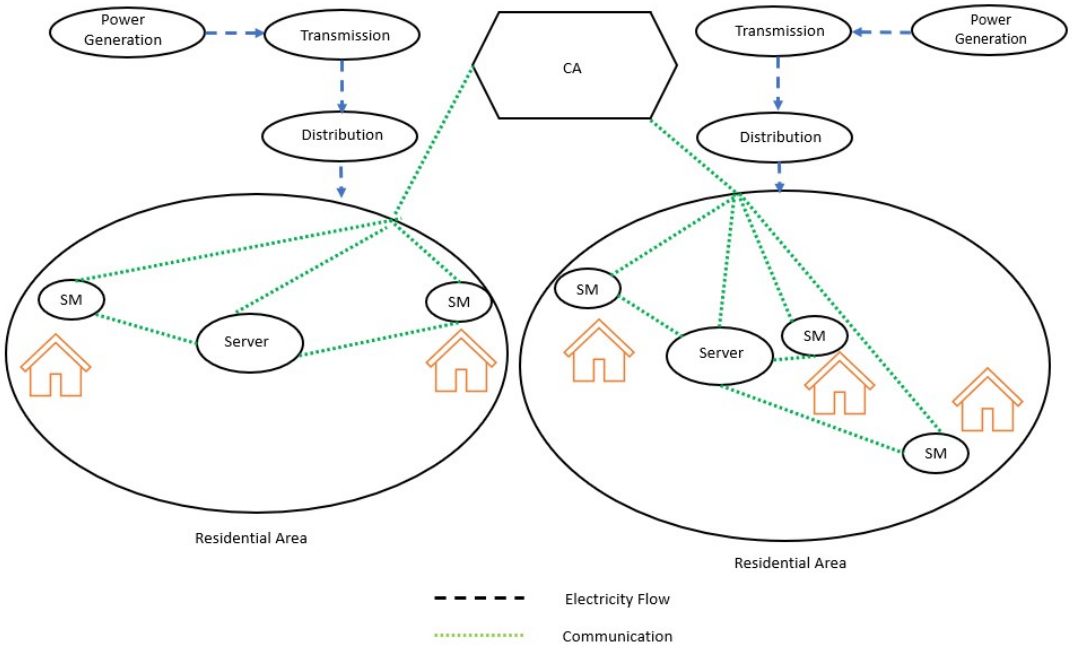

Fig. 1. System model.

B. Adversary Model

Since the smart meters communicate to the server through an insecure medium (the Internet), an adversary may carry out various attacks on the communication channels. We assume the widely accepted Dolev-Yao model (DY model) [50] and CK adversary model [51], [52]. In the DY adversary model, an adversary may listen, modify, intercept, or replay the transmitted messages. Also, the adversary can capture long-term secrets (keys that are used across multiple sessions) or short-term keys [51], [52] in the CK model. A protocol is secure under CK model if it is not vulnerable to both long-term and ephemeral secrets disclosure attacks [53]. In other words, to be CK-secure, the protocol must have perfect forward secrecy and ephemeral secret leakage attack resistance [18], [51].

We also assume that the adversary may have quantum computing capabilities, in which case he/she may break the security of certain classical systems by employing quantum algorithms.

C. Security Goals

In this subsection, we list the security goals for the proposed protocol.

Protection From Conventional and Quantum Computer-Enabled Attacks: The security solutions for smart meter communications should provide protection against conventional attacks such as eavesdropping, replay, and impersonation attacks. Such solutions should also provide protection against future attacks by an adversary with quantum computing capabilities.

Mutual Authentication: The smart meters send their readings of energy consumption to the server through an insecure channel, the Internet. Both parties must ensure that they are communicating with the right party on the other side. Hence, mutual authentication is essential before the data transfer.

Session Key: The smart meters send their readings of energy consumption to the server. This communication needs to be secured through the establishment of a session key.

Perfect forward secrecy (PFS): A protocol with PFS ensures that past established session keys remain secure even if long-term secret keys are exposed [18], [51]. An adversary can capture all exchanged messages and wait for long-term secret key leakage. If the protocol does not offer PFS, the captured messages can be decrypted using session keys generated from the leaked keys. To have PFS, session random secrets must also be used to compute the session key [18].

Ephemeral secret leakage (ESL) resistance: A protocol with ephemeral secret leakage resistance ensures session key security even if ephemeral secrets are exposed [53].

Known key secrecy: The protocol must ensure that even if an adversary can get a session key, he/she should not get past or future session keys [18].

Strong anonymity: This is an important security goal to maintain the privacy of protocol participants. There are two types of anonymity, weak and strong. If a pseudo-identity is used instead of the real identity of the user, the protocol offers anonymity [18]. However, if the same pseudo-identity is used in all the sessions of the protocol, an adversary can link the messages. Hence, such a protocol that uses the same pseudo-identity for a participant offers only weak anonymity. The pseudo-identity should be changed in each iteration of the protocol so that the messages are unlinkable and the protocol offers strong anonymity [18].

Unlinkability: An adversary should not be able to link a message to the entity that created the message. The adversary

also should not be able to link two sessions of the protocol. To achieve this goal, the parameters used in each session (e.g., pseudo-identities) should be changed.

Privacy: The energy consumption data and usage patterns should not be available to an attacker in order to preserve the privacy of customers. Even if an attacker listens to the exchanged messages, he/she must not be able to link them to any customer.

IV. Proposed Authentication Protocol

We present the proposed authentication scheme in this section. The high-level workflow of the authentication scheme is illustrated in Figure 2. This figure demonstrates how the secure key from QKD and true random numbers from QRNG are integrated into the proposed protocol. A secure key is established between the smart meter and the server through QKD with the help of the $\mathcal{CA}$. The QRNG provides true, secure random numbers to the smart meter and the server. The secure key generated through the QKD process and the QRNG-generated random numbers are used during mutual authentication, and a session key is established between the smart meter and the server.

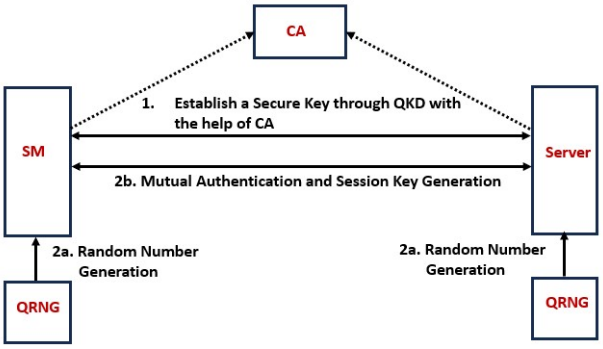

Fig. 2. The high-level workflow of the authentication scheme.

The proposed protocol consists of three phases: registration, mutual authentication, and QKD update. The registration phase is required to be executed only once. The mutual authentication phase is carried out whenever the smart meter wants to send information to the server. This is followed by the QKD update phase to update the key established between the smart meter and the server.

The notations used in the proposed protocol and their descriptions are given in Table II.

A. Assumptions

- Each smart meter is equipped with a QRNG. There is a QRNG in the server as well.
- The smart meters and the server are installed with QKD transmitters.
- A fiber optic cable exists between the central authority and smart meters as well as between the central authority and servers to enable quantum information transmission.

TABLE II
Table of Notations

Notation	Description
QKD	Quantum Key Distribution
$QRNG$	Quantum Random Number Generator
$\mathcal{SM}_x$	Smart Meter
ID	Real identity of $\mathcal{SM}_x$
ID_p	Pseudo-id of $\mathcal{SM}_x$
$\mathcal{S}$	Server
$\mathcal{CA}$	Central authority
K_x	Ky established through QKD
A	Adversary
R_i, N_i	Random numbers generated using QRNG
SK_i	Session key
α_1, α_2	Hash parameters
$\|$	Concatenation operation
$\oplus$	XOR operation
$h(X)$	Hash of X
M_n	n^{th} Authentication Message

B. Registration Phase

The steps involved in the smart meter registration phase are as follows:

Step 1: A smart meter $\mathcal{SM}_x$ with a real identity ID sends a registration request to the $\mathcal{CA}$. The $\mathcal{CA}$ generates a pseudo-ID, ID_p, for $\mathcal{SM}_x$ and stores ID_p in its database. The $\mathcal{CA}$ also assigns a server $\mathcal{S}$ to $\mathcal{SM}_x$. $\mathcal{SM}_x$ will be communicating with $\mathcal{S}$. Then, $\mathcal{CA}$ sends ID_p to $\mathcal{SM}_x$ and ID_p and ID to $\mathcal{S}$.

Step 2: $\mathcal{SM}_x$ and $\mathcal{S}$ prepare quantum states independently, based on their random choices of systems settings, including intensity selection, basis selection, and a random bit. $\mathcal{SM}_x$ generates n states as $\{a*_{x1}, a*_{x2}, \ldots, a*_{xn}\}$ and $\mathcal{S}$ generates n states as $\{b*_{x1}, b*_{x2}, \ldots, b*_{xn}\}$. After that, $\mathcal{SM}_x$ and $\mathcal{S}$ send the prepared quantum states to the $\mathcal{CA}$ over the quantum channel.

Step 3: $\mathcal{SM}_x$, $\mathcal{S}$, and $\mathcal{CA}$ follow the steps mentioned in Section II-B to derive a symmetric key. Let there be m retained bits from the measurements denoted as $\{a_{x1}, a_{x2}, \cdots, a_{xm}\}$. Thus, a key $K_x = a_{x1}a_{x2}\ldots a_{xm}$ is established through the QKD process between $\mathcal{SM}_x$ and $\mathcal{S}$.

C. Mutual Authentication Phase

The steps involved in the i^{th} round of the execution of the authentication phase between $\mathcal{SM}_x$ and the server $\mathcal{S}$ are described below:

Step 1: $\mathcal{SM}_x$ generates a random number R_i of length n using the QRNG. Then, $\mathcal{SM}_x$ computes R_i^* by performing the XOR operation on R_i with K_x as:

$$R_i^* = R_i \oplus K_x. \tag{2}$$

Subsequently, $\mathcal{SM}_x$ computes a hash parameter α_1 as

$$\alpha_1 = h(R_i^* \parallel K_x). \tag{3}$$

After that, $\mathcal{SM}_x$ composes a message M_1 with a data transfer request, its pseudo-identity ID_p, R_i^*, and α_1 as $M_1 = \{Req, ID_p, R_i^*, \alpha_1\}$ and sends M_1 to $\mathcal{S}$.

TABLE III
MUTUAL AUTHENTICATION BEFORE DATA TRANSFER

Smart Meter		Server
Generate: $R_i = QRNG()$		
$R_i^* = R_i \oplus K_x$		
$\alpha_1 = h(R_i^* \parallel K_x)$		
$M_1 = \{Req, ID_p, R_i^*, \alpha_1\}$		
	$\xrightarrow{M_1}$	
		Verify: ID_p
		Retrieve: K_x
		$R_i = R_i^* \oplus K_x$
		Compute and Verify: $\alpha_1 = h(R_i^* \parallel K_x)$
		Generate: $N_i = QRNG()$
		$N_i^* = N_i \oplus K_x$
		Generate: ID_p^{new}
		$ID_p^{*new} = ID_p^{new} \oplus R_i$
		Compute: $SK_i = h(ID \parallel ID_p \parallel R_i \parallel N_i \parallel K_x)$
		Store: SK_i
		$\alpha_2 = h(N_i^* \parallel K_x)$
		$M_2 : \{Ack, N_i^*, ID_p^{*new}, \alpha_2\}$
	$\xleftarrow{M_2}$	
Decode: $N_i = N_i^* \oplus K_x$		
Compute and Verify: $\alpha_2 = h(N_i^* \parallel K_x)$		
$ID_p^{new} = ID_p^{*new} \oplus R_i$		
Store: ID_p^{new}		
Compute: $SK_i = h(ID \parallel ID_p \parallel R_i \parallel N_i \parallel K_x)$		
Store: SK_i		

Step 2: After receiving M_1, $\mathcal{S}$ verifies whether ID_p exists in its database and retrieves K_x that was established with SM_x through the QKD process in the registration phase. Then, $\mathcal{S}$ computes R_i from R_i^* as:

$$R_i = R_i^* \oplus K_x. \tag{4}$$

After that, $\mathcal{S}$ computes and verifies the hash parameter α_1 as

$$\alpha_1 = h(R_i^* \parallel K_x). \tag{5}$$

After verifying α_1, $\mathcal{S}$ generates a random number N_i of length n using the QRNG. Then, $\mathcal{S}$ computes N_i^* by performing the XOR operation on N_i with K_x as:

$$N_i^* = N_i \oplus K_x. \tag{6}$$

Subsequently, $\mathcal{S}$ generates a new ID, ID_p^{new}, for the smart meter to use in the next iteration of the authentication session and generates ID_p^{*new} by performing the XOR operation on ID_p^{new} with R_i as:

$$ID_p^{*new} = ID_p^{new} \oplus R_i. \tag{7}$$

$\mathcal{S}$ generates the session key SK_i as $SK_i = h(ID \parallel ID_p \parallel R_i \parallel N_i \parallel K_x)$ and stores it. After that, $\mathcal{S}$ computes a hash parameter α_2 as

$$\alpha_2 = h(N_i^* \parallel K_x). \tag{8}$$

Then, $\mathcal{S}$ composes a message M_2 with an acknowledgement, N_i^*, ID_p^{*new}, and α_2 as $M_2 = \{Ack, N_i^*, ID_p^{*new}, \alpha_2\}$ and sends M_2 to $\mathcal{SM}_x$.

Step 3: When $\mathcal{SM}_x$ receives M_2, it first extracts N_i^* and decodes N_i from N_i^* as:

$$N_i = N_i^* \oplus K_x. \tag{9}$$

After that, $\mathcal{S}$ computes and verifies the hash parameter α_2 as

$$\alpha_2 = h(N_i^* \parallel K_x). \tag{10}$$

If the verification is successful, $\mathcal{SM}_x$ decodes ID_p^{new} by performing the XOR operation on ID_p^{*new} with R_i as:

$$ID_p^{new} = ID_p^{*new} \oplus R_i. \tag{11}$$

$\mathcal{SM}_x$ stores the new ID, ID_p^{new}, to use in the next iteration of the authentication session. Then, $\mathcal{SM}_x$ generates the session key SK_i as $SK_i = h(ID \parallel ID_p \parallel R_i \parallel N_i \parallel K_x)$ and stores it. Thus, a session key is established between $\mathcal{SM}_x$ and $\mathcal{S}$ for secure communication. The i^{th} round of mutual authentication is illustrated in Table III.

D. QKD Update Phase

$\mathcal{SM}_x$ and $\mathcal{S}$ prepare quantum states independently and send the prepared quantum states to the $\mathcal{CA}$ over the quantum channel. Then, $\mathcal{SM}_x$, $\mathcal{S}$, and $\mathcal{CA}$ follow the steps mentioned in Section II-B to derive a symmetric key and update K_x. The new K_x will be used in the next round of the authentication phase. Thus, K_x is not reused.

V. SECURITY ANALYSIS

A. Formal Security Analysis

In this subsection, we provide formal proof of the proposed protocol using the Real-Or-Random (RoR) model [54].

Security Model: An adversary A's aim is to distinguish the established session key in a protocol session between the smart meter and the server [53]. A interacts with the smart meter and the server by calling the following oracle queries:

- *Execute($\mathcal{SM}_x$, $\mathcal{S}$):* This query is used to model a passive attack where $\mathcal{A}$ listens to the transmitted messages.

- *Send(X, m):* This query is used to model an active attack. When $\mathcal{A}$ executes *Send(X, m)*, a message m will be sent to X where X is a smart meter or server.
- *Hash(m):* This query is used to obtain the hash of a message m.
- *Reveal(X):* $\mathcal{A}$ calls *Reveal(X)* query to capture the ephemeral secrets of X where X is a smart meter or server. This query models the ephemeral secret leakage attack.
- *Corrupt(X):* $\mathcal{A}$ calls *Corrupt(X)* query to capture the long-term secret credential of X.
- *Test():* This query defines the session key's semantic security. $\mathcal{A}$ can call this query only once. When $\mathcal{A}$ runs *Test()*, a bit b will be flipped. If $b = 1$, the actual session key is returned to $\mathcal{A}$. If $b = 0$, $\mathcal{A}$ receives a random string.

Definition 1: If $Pr[Succ_A]$ denotes the probability that A wins the game, the advantage of A in breaking the semantic security of the proposed scheme is is $Adv_A = \mid 2Pr[Succ_A] - 1 \mid$. If Adv_A is negligible, the protocol is secure against the CK-adversary under the random oracles [53].

Definition 2: Quantum cryptography relies on the fundamental principles of quantum physics to enable secure communication among distant parties. Specifically, the no-cloning theorem forbids the creation of an exact copy of an arbitrary unknown quantum state [55], and the monogamy of quantum entanglement states that if two parties share a maximally entangled state, they cannot be correlated with any third party. These quantum mechanical properties allow QKD protocols to be designed with provable security. In this case, the advantage of $\mathcal{A}$ in getting the secret keys can be upper-bounded by an arbitrarily small probability ϵ, i.e., $Adv_A^{QKD} \leq \epsilon$.

Theorem 1. Let A be an adversary attempting to break the semantic security of the proposed protocol. Let q_h, q_s, and q_e represent the number of Hash, Send, and Execute queries, respectively. Let $|H|$ denote the hash output's length and let Adv_A^{QKD} denote A's advantage in getting the key established through the QKD process. Then, the advantage of A winning against the proposed protocol is $Adv_A \leq \frac{(q_h)^2}{2^{(H-1)}} + \frac{(q_s+q_e)^2}{p} + \frac{q_s}{2^{(H-1)}} + 2q_h Adv_A^{QKD}$ which is negligible.

Proof: We consider a series of games G_i for $i \in \{0, 1, 2, 3, 4, 5\}$.

Game G_0**:** G_0 represents a real attack by A against the protocol. Since A guesses the bit b randomly in G_0, according to Definition 1, the advantage of A in guessing b is:

$$Adv_A = \mid 2Pr[Succ_{A,G_0}] - 1 \mid . \tag{12}$$

Game G_1**:** In this game, all queries are simulated. Since Execute, Send, and the rest of the queries are simulated as in a real attack, games G_0 and G_1 are identical and we can write that:

$$Pr[Succ_{A,G_1}] = Pr[Succ_{A,G_0}]. \tag{13}$$

Game G_2**:** The simulation of G_2 is same as G_1 except that G_2 will be stopped if there are collisions in hash or transcripts. If there is no collision, G_1 and G_2 are indistinguishable. From the birthday paradox, the probability of hash collision is at most $\frac{(q_h)^2}{2^{(H+1)}}$ and the collision probability in transcripts is $\frac{(q_s+q_e)^2}{2p}$ where p is the length of the transcripts [26], [53]. Hence, we can write that:

$$Pr[Succ_{A,G_2}] - Pr[Succ_{A,G_1}] \leq \frac{(q_h)^2}{2^{(H+1)}} + \frac{(q_s+q_e)^2}{2p}. \tag{14}$$

Game G_3**:** The simulation of G_3 is same as G_2 except that G_3 will be stopped if A can guess the verifier's value correctly without sending the $Hash()$ oracle. This happens only by sending $Send()$ queries. Hence, we can write:

$$Pr[Succ_{A,G_3}] - Pr[Succ_{A,G_2}] \leq \frac{q_s}{2^{(H)}}. \tag{15}$$

Game G_4**:** This game considers two scenarios of session key leakage. In the first scenario corresponding to the PFS feature, A calls $Corrupt()$ query to get the long-term secret (the identity of the smart meter, ID). In the second case corresponding to the ESL attack resilience, A calls the $Reveal()$ query to get the ephemeral random numbers (N_i and R_i). However, the session key is calculated as $SK_i = h(ID \parallel ID_p \parallel R_i \parallel N_i \parallel K_x)$. Without knowing K_x (the key established through the QKD process), A cannot compute the session key SK_i. By Definition 2, the no-cloning theorem forbids the creation of an exact copy of an arbitrary unknown quantum state. Also, due to the principles of quantum entanglement, if two parties share a maximally entangled state, they cannot be correlated with any third party. As a result, the difference between G_3 and G_4 is negligible as per Definition 2. Hence, we can write that:

$$Pr[Succ_{A,G_4}] - Pr[Succ_{A,G_3}] \leq q_h Adv_A^{QKD}. \tag{16}$$

Game G_5**:** The difference between this game and G_4 is that in this game, A sends a $Hash()$ query. Since A can reach the session key with a probability of $\frac{(q_h)^2}{2^{(H+1)}}$, we can write that:

$$Pr[Succ_{A,G_5}] - Pr[Succ_{A,G_4}] \leq \frac{(q_h)^2}{2^{(H+1)}}. \tag{17}$$

If A has executed all the above games to break the security of the protocol and has not had a successful attempt, A guesses the bit b and calls the $Reveal()$ query to win the game as the final attempt. Then, we can write that:

$$Pr[Succ_{A,G_5}] = \frac{1}{2}. \tag{18}$$

Combining (12) and (13), we can write the following:

$$\begin{aligned} \frac{1}{2}Adv_A &= \mid Pr[Succ_{A,G_0}] - \frac{1}{2} \mid \\ &= \mid Pr[Succ_{A,G_1}] - \frac{1}{2} \mid . \end{aligned} \tag{19}$$

Using Equations (14) to (19) and by applying the triangle inequality, we have:

$$\begin{aligned}\frac{1}{2}Adv_A &= \mid Pr[Succ_{A,G_1}] - \frac{1}{2} \mid \\ &= \mid Pr[Succ_{A,G_1}] - Pr[Succ_{A,G_5}] \mid \\ &\leq \frac{(q_h)^2}{2^{(H)}} + \frac{(q_s+q_e)^2}{2p} + \frac{q_s}{2^{(H)}} + q_h Adv_A^{QKD} \quad (20)\end{aligned}$$

By multiplying both sides of Equation (20) by 2, we get:

$$Adv_A \leq \frac{(q_h)^2}{2^{(H-1)}} + \frac{(q_s+q_e)^2}{p} + \frac{q_s}{2^{(H-1)}} + 2q_h Adv_A^{QKD}. \quad (21)$$

■

B. Informal Security Analysis

Protection Against Quantum Computer-Enabled Attacks: Conventional asymmetric cryptographic techniques make the assumption that the underlying mathematical problems are complex and cannot be solved by an adversary efficiently. However, such mathematical problems could be solved efficiently with algorithm and hardware development. Hence, the security of the conventional cryptographic protocols used in smart meter communications could be compromised by quantum computer-enabled adversaries.

In the proposed protocol, a secret key is derived through the QKD process. Unlike the conventional asymmetric cryptographic techniques, QKD is not based on the assumption of the complexity of the underlying mathematical concepts and the adversary's inability to solve them efficiently. QKD establishes secure keys between two parties by making use of the principles of quantum mechanics. As a result, even if the attacker has quantum computing capabilities, the security offered by the proposed protocol is not affected. Thus, the proposed protocol provides protection against quantum computer-enabled attacks.

Perfect Forward Secrecy: In the proposed protocol, the session key is computed as $SK_i = h(ID \parallel ID_p \parallel R_i \parallel N_i \parallel K_x)$. Ephemeral random numbers generated by QRNG, R_i and N_i, and the key established through QKD, K_x, are used in the computation of the session key SK_i. Hence, even if the long-term credential, ID, is leaked, the adversary cannot calculate the previous session keys because he/she must know R_i, N_i, and K_x, to compute previous session keys.

Ephemeral secret leakage attack resistance: In the proposed protocol, the session key is computed as $SK_i = h(ID \parallel ID_p \parallel R_i \parallel N_i \parallel K_x)$. Long-term credential, ID, and the key established through QKD, K_x, are used in the computation of the session key SK_i. Hence, even if the ephemeral secrets R_i and N_i are disclosed, the adversary cannot calculate the session keys because he/she must know ID and K_x to compute session keys. Thus, even if the ephemeral secrets are disclosed to an adversary, the session key is secure in the proposed protocol.

Known Key Secrecy: In the proposed protocol, the session keys in different sessions are independent of each other. Suppose an adversary gets access to a session key from the i^{th} session in the proposed protocol. The session key for the i^{th} session computed as $SK_i = h(ID \parallel ID_p \parallel R_i \parallel N_i \parallel K_x)$. To derive a session key for another session j, the adversary must know the QRNG-generated random numbers (R_j and N_j), the long-term credential (ID), and the key established through QKD for session j. Since they are not available to the adversary, the session key for session j is not compromised. Hence, even if the adversary gets access to a session key, he/she cannot derive past or future session keys from the disclosed session key. Thus, the proposed protocol offers known key secrecy.

Strong Anonymity: A pseudo-id is used during the authentication phase, thereby maintaining the anonymity of the smart meter. Further, the pseudo-identity of the smart meter is changed in each iteration of the protocol so that the messages are unlinkable. Thus, the protocol offers strong anonymity.

Protection Against Eavesdropping Attacks: Since there are two channels used in the proposed protocol, we analyze eavesdropping on each channel separately. Suppose the attacker tries to eavesdrop on the quantum channel. Due to the principles of quantum mechanics, such an attempt will be noticed by the participants. If the attacker eavesdrops on the classical channel, since the messages are XORed with the secret key established through the QKD process, the attacker will not be able to decode and understand the messages. As a result, the proposed protocol protects against eavesdropping attacks.

Protection Against Replay Attacks: The pseudo-id and the random number from the smart meter are changed during each authentication session. Hence, an adversary cannot replay a captured message M_1 later. Similarly, the adversary also cannot replay M_2 as a new random number is generated by the server in each session. As a result, the adversary cannot replay the previous messages successfully.

Protection Against Impersonation Attacks: Consider the scenario where an adversary attempts to impersonate a smart meter $\mathcal{SM}_x$. To impersonate $\mathcal{SM}_x$, the adversary must compose a valid message M_1 using the secret key K_x. K_x is established between $\mathcal{SM}_x$ and $\mathcal{S}$ through the QKD process by sending photons. Eavesdropping on the photons in an attempt to derive the key will expose the attacker, as per the principles of quantum mechanics. Hence, K_x is not accessible to the adversary to compose valid messages. As a result, the protocol protects against impersonation attacks.

Mutual Authentication: Only a legitimate smart meter and server that derive a symmetric key through the QKD process can generate valid messages to get authenticated. Thus, the proposed protocol enables mutual authentication between a legitimate smart meter and a server.

Unlinkability: The pseudo-id of the smart meter is used in the proposed protocol instead of its real identity. Further, it is unique for each authentication event which ensures unlinkability between two sessions of the same smart meter.

Privacy: Even if an adversary listens to the exchanged messages, he/she cannot link them to any customer due to the anonymity and unlinkability properties discussed above. Hence, the energy consumption data and usage patterns are not available to an attacker, thereby preserving the privacy of customers.

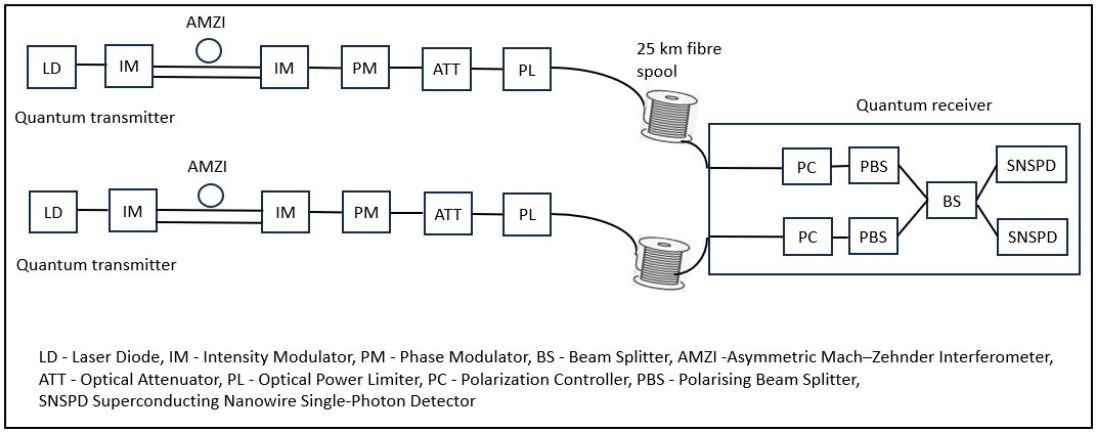

Fig. 3. Schematic diagram of the MDI QKD.

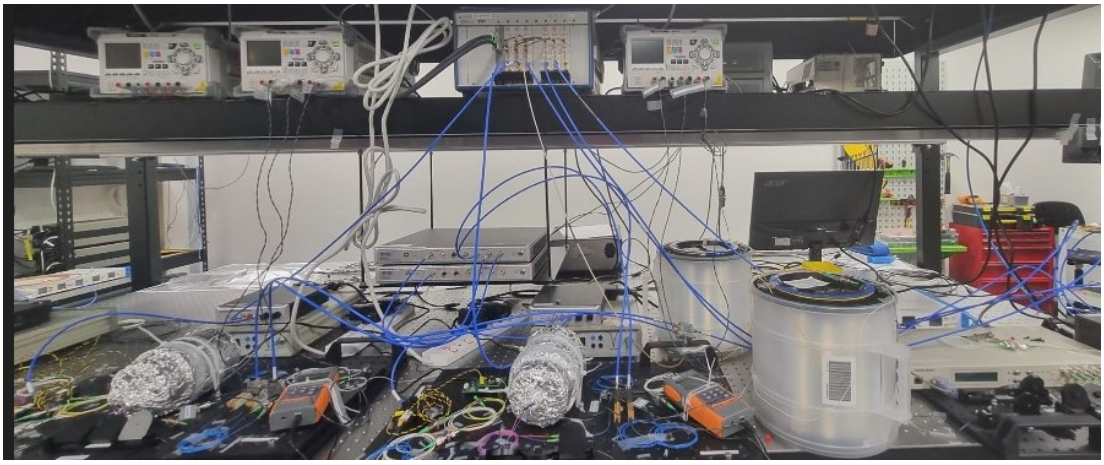

Fig. 4. Experimental setup of the MDI QKD.

Session Key Security: The proposed protocol enables the generation of a session key between $\mathcal{SM}_x$ and $\mathcal{S}$ as $SK_i = h(ID \parallel ID_p \parallel R_i \parallel N_i \parallel K_x)$. Only a legitimate smart meter and server know the parameters required to generate SK_i. Thus, the proposed protocol provides session key security.

VI. Experimental Details of the Protocol Implementation

In this section, we present the details of an experimental evaluation of the proposed protocol with MDI QKD and QRNG systems. First, we describe the overall experimental setup. Then, we present each system of the setup in detail.

The schematic diagram of the experimental setup follows Figure 2. The two primary systems in the proposed scheme are the MDI QKD system and the QRNG system. The secret keys from the QKD system and random numbers from the QRNG system are required inputs for mutual authentication. In the MDI QKD system, quantum transmitters are paired for key distribution. This process involves quantum state preparation, quantum state measurement, and classical post-processing. The QRNG system consists of quantum state emission and homodyne detection. The smart meter and the server authenticate each other using the secret keys from the MDI QKD system and the random numbers from the QRNG system. In our experimental settings, we implement the quantum parts of the protocol (the MDI QKD system and the QRNG system) as described below.

A. MDI QKD System

The workflow of the MDI QKD is provided in Section II-B. We follow the experimental settings of MDI QKD implementations, including the quantum layer and post-processing as provided in [24]. The schematic diagram of the MDI QKD system is depicted in Figure 3, illustrating secure key distribution between two distant parties ($\mathcal{SM}_x$ and $\mathcal{S}$). Each party holds a quantum transmitter, randomly preparing quantum states and sending them to an untrusted third party, $\mathcal{CA}$, who serves as the quantum receiver for quantum state measurement.

In the quantum transmitters, coherent states are produced by driving a distributed-feedback (DFB) laser diode in gain-switching mode. This ensures that each generated laser pulse has an intrinsically random and independent phase, essential for decoy-state analysis [56]–[58]. Additionally, an asymmetric Mach-Zehnder interferometer (AMZI), Intensity Modulator (IM), and Phase Modulator (PM) are used to modulate the photon into time-bin phase-encoded quantum

states $|e\rangle$, $|l\rangle$, $(|e\rangle + |l\rangle)/\sqrt{2}$ and $(|e\rangle - |l\rangle)/\sqrt{2}$. Here, e and l represent early and late time-bin, respectively.

Furthermore, the photons are carefully calibrated in all degrees of freedom, including central wavelength with a precision of 0.1 pm, timing precision of 10 ps, and fine-tuning of the state of polarization at the receiver side. A Hong-Ou-Mandel interference visibility measurement of 0.48 indicates good mode overlap of the independently generated photons, ensuring an efficient Bell-state-measurement (BSM) for our MDI QKD system.

Then, the quantum states travel through a 25 km spooled optical fibre to the quantum receiver. At the receiver's side, the quantum efficiency of the measurement devices is characterized to be 70.73%, on average. After receiving the quantum states, $\mathcal{CA}$ publicly announces the BSM results. $\mathcal{SM}_x$ and $\mathcal{S}$ then perform corresponding classical data post-processing, including basis sifting, error correction, and privacy amplification, to obtain the final secure keys. We run the system at a repetition rate of 125 MHz and generate 6.5×10^5 bits of final secure keys and use 128 bits for K_x for demonstration.

B. QRNG System

To generate the random numbers, we employ the methodology of the QRNG system in [49]. The schematic diagram for generating random numbers is shown in Figure 5.

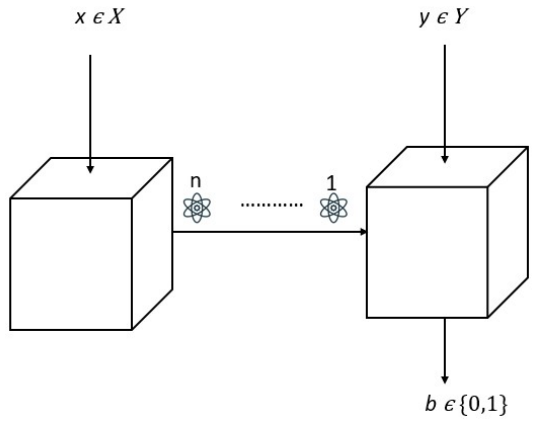

Fig. 5. Schematic diagram of the QRNG experimental setup.

The QRNG system consists of two key components: quantum state preparation and quantum state measurement. In the quantum state preparation phase, coherent states undergo modulation in the Quadrature Phase Shift Keying (QPSK) format based on the random variable x (which is operated by Alice). These states are subsequently measured by an uncharacterized balanced homodyne detector (which is operated by Bob), with the choice of basis determined by y, yielding the outcome denoted by b.

Based on the prepare-and-measure (P&M) configuration [49], we designed a self-testing QRNG protocol where the working of Bob's measurement device is not assumed a priori. However, it can be verified using experimental statistics. To be more specific, every round of the experiment is randomly assigned to be a generation round or test round. During the test round, the device plays a P&M game $\mathcal{G}$, where Alice and Bob perform quantum state preparation and measurement based on a prefixed probability distribution $q(x, y)$. For each pair of inputs x and y, the game $\mathcal{G}$ defines the winning outcome $b_{xy} \in \{0, 1\}$. For a given round, the device wins the game if Bob outputs the winning outcome. In the generation round, Alice and Bob choose a specific x and y combination. We follow the systematic method to choose the winning outcome $b_{xy} \in \{0, 1\}$ and the probability distribution $q(x, y)$ as given in [49].

The amount of entropy in our QRNG protocol is analyzed mainly by characterizing the quantum correlations using a semidefinite programming (SDP) technique developed in [59]. The security analysis guarantees that after successful execution of the protocol, the output string is close to an ideal random bit-string that is uniformly random and independent from any pre-shared quantum (and also classical) information held by any adversary or observer.

In the experiment, we use an external cavity semiconductor laser with a central wavelength of 1550 nm and a linewidth of 50 kHz. It is divided into two paths, one for quantum state preparation and the other as Local Oscillator (LO) for balanced homodyne detection. In the signal path, an Intensity Modulator (IM) first curves the continuous-wave (c.w.) laser into pulses with a pulse width of 4 ns each, for defining the temporal mode of the quantum states. A Phase Modulator (PM) modulates the phase of the quantum states. After that, an optical attenuator attenuates the signals to single-photon energy level to finally generate the QPSK quantum states $\{|\alpha e^{ixpi/2}\rangle\}$ where $x \in \{0, 1, 2, 3\}$.

In the quantum state measurement, a high-efficiency and low-noise fibre-coupled homodyne detector is deployed. The overall efficiency of the photodiodes including the coupling loss is measured to be 98.3% and 98.8%, respectively. The 3 dB bandwidth of the homodyne detector is 72 MHz, and the clearance (shot noise to electronic noise ratio) is 16.94 dB with a 10 mW LO. Thus, we generate 128 bits of random numbers for R_i and N_i.

VII. Performance Analysis

In this section, we compare the proposed protocol with other existing protocols in terms of the achieved security properties. Subsequently, we analyze the computation cost of the proposed protocol and compare it with the computation cost of other protocols.

A. Comparison of Security Properties

A summary of the comparison of the security features is given in Table IV. The main security feature that differentiates the proposed protocol from other protocols is that it can provide protection against quantum computer-enabled attacks. In addition, the proposed protocol offers mutual authentication between the smart meter and the server, anonymity, privacy, session key security, perfect forward secrecy, known key secrecy, unlinkability, ephemeral secret leakage attack resistance, and protection from replay, impersonation, and eavesdropping attacks. It can be noted that

TABLE IV
COMPARISON BASED ON SECURITY FEATURES

Scheme	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12
Abbasinezhad-Mood and Nikooghadam [26]	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Srinivas et al. [27]	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Odelu et al. [28]	N	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y
Wu et al. [29]	N	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N
Garg et al. [30]	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Mahmood et al. [32]	N	Y	Y	Y	Y	Y	Y	Y	N	N	Y	N
Abbasinezhad-Mood and Nikooghadam [33]	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
Proposed Protocol	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
S1: Protection against quantum computer-enabled attacks; **S2:** Mutual authentication; **S3:** Session key;												
S4: Replay attack protection; **S5:** Protection against impersonation attacks; **S6:** Eavesdropping attack protection;												
S7: Anonymity; **S8:** Privacy; **S9:** Perfect forward secrecy; **S10:** Known key secrecy; **S11:** Unlinkability; **S12:** ESL resistance												

TABLE V
COMPUTATION COST DURING AUTHENTICATION

Scheme	Smart Meter	Server/Service Provider
Abbasinezhad-Mood and Nikooghadam [26]	$5t_h + 4t_{ecm} + t_{eca} = 5.23$ ms	$5t_h + 4t_{ecm} + t_{eca} = 5.23$ ms
Srinivas et al. [27]	$7t_h + 3t_{ecm} + t_{eca} = 4.08$ ms	$7t_h + 3t_{ecm} + t_{eca} = 4.08$ms
Odelu et al. [28]	$6t_h + 3t_{ecm} + t_{exp} = 4.37$ ms	$6t_h + 2t_{ecm} + t_{exp} + 2t_{bp} = 9.52$ms
Wu et al. [29]	$3t_{ecm} + t_s + t_m + 5t_h = 5.64$ ms	$3t_{ecm} + t_s + t_m + 6t_h = 5.65$ ms
Garg et al. [30]	$2t_{ecm} + 4t_h = 2.38$ ms	$2t_{ecm} + 4t_h = 2.38$ ms
Mahmood et al. [32]	$3t_{eca} + 5t_{ecm} + 3t_h = 7.38$ ms	$3t_{eca} + 5t_{ecm} + 4t_h = 7.39$ms
Abbasinezhad-Mood and Nikooghadam [33]	$4t_h + 4t_{ecm} + 2t_{eca} = 5.72$ ms	$4t_h + 4t_{ecm} + 2t_{eca} = 5.72$ ms
Proposed Scheme	$3t_x + 6t_c + 3t_h = 0.108$ ms	$3t_x + 6t_c + 3t_h = 0.108$ ms

some other existing schemes do not meet all the imperative security properties.

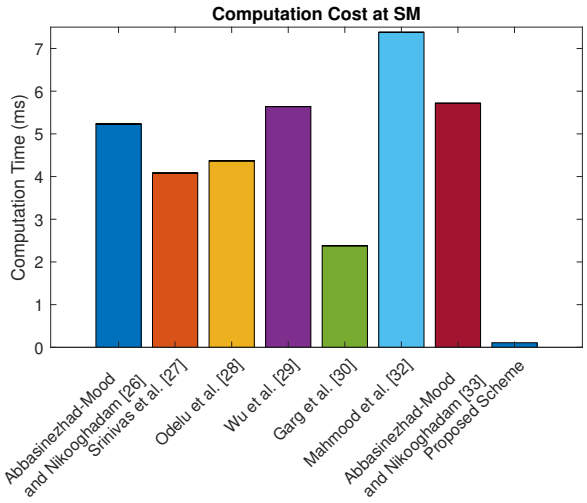

Fig. 6. Computation cost at the SM.

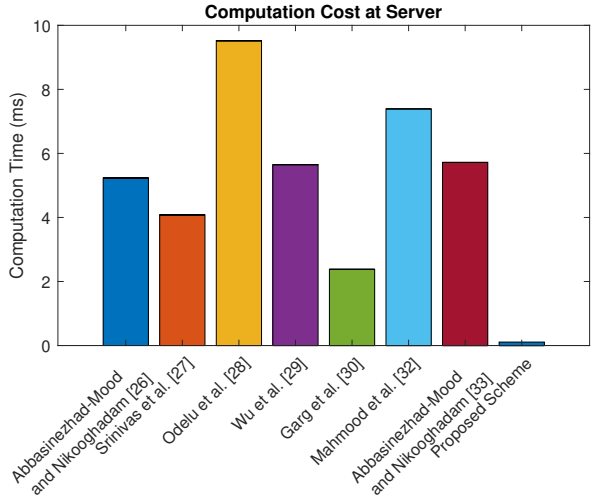

Fig. 7. Computation cost at the server.

B. Computation Cost

Next, we analyze the proposed protocol's computation cost by computing the execution time incurred during the authentication phase. Then, we compare it with that of four recent protocols. The proposed protocol only uses lightweight operations. We consider the experiment settings and results mentioned in [27] using the Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL) on Intel Pentium i4 processor with 512 MB RAM @ 3 GHz. In our analysis, t_x, t_c, t_{ecm}, t_{eca}, t_s, t_m, t_{exp}, t_{bp}, and t_h represent the time taken for XOR, concatenation, ECC point multiplication, ECC point addition, double scalar multiplication, modular multiplication, modular exponentiation, bilinear pairing, and one-way hash operations, respectively. From the experiments, $t_x = 0.008$ ms, $t_c = 0.009$ ms, $t_{ecm} = 1.17$ ms, $t_{eca} = 0.5$ ms, $t_s = 2.05$ ms, $t_m = 0.03$ ms, $t_{exp} = 0.8$ ms, $t_{bp} = 3.16$ ms, and $t_h = 0.01$ ms. The comparison results are summarised in Table V. We have also plotted the computation costs incurred during the authentication phases at the smart meter and the server in Figures 6 and 7, respectively. The performance comparison based on the total computation cost at the smart meter and server during the authentication phase is plotted in Figure 8. From Figures 6, 7, and 8, it can be concluded that the

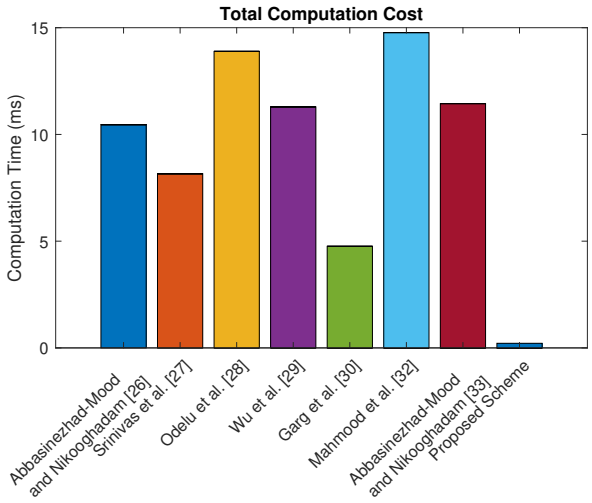

Fig. 8. Total computation cost.

computation time for the proposed protocol is lower than other schemes.

VIII. Conclusion

It is imperative to replace conventional cryptography systems with quantum-safe ones given the acceleration of quantum computing research. One such scenario which requires quantum-safe protocols is smart meter communications. In this paper, we proposed a quantum-safe authentication protocol for smart meter communications. Further, we demonstrated the feasibility of the proposed protocol by deploying an MDI QKD system and a QRNG system. Through formal and informal security proofs of the proposed protocol, we have demonstrated that the proposed protocol is secure against classical as well as quantum computer-enabled attacks. Our performance analysis shows that the computation cost of the proposed protocol is lower than other schemes for smart meter communications. We can conclude that the proposed protocol offers better security protection at a lower cost.

IX. Acknowledgement

This research was supported by the National Research Foundation, Singapore and A*STAR under its Quantum Engineering Programme (National Quantum-Safe Network, NRF2021-QEP2-04-P01).

References

[1] N. Saxena and B. J. Choi, "State of the art authentication, access control, and secure integration in smart grid," *Energies*, vol. 8, no. 10, pp. 11 883–11 915, 2015.

[2] D. Abbasinezhad-Mood and M. Nikooghadam, "An ultra-lightweight and secure scheme for communications of smart meters and neighborhood gateways by utilization of an arm cortex-m microcontroller," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6194–6205, 2018.

[3] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Başar, "Demand response management in the smart grid in a large population regime," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 189–199, 2015.

[4] M. H. Rehmani, M. Reisslein, A. Rachedi, M. Erol-Kantarci, and M. Radenkovic, "Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 2814–2825, 2018.

[5] N. Javaid, G. Hafeez, S. Iqbal, N. Alrajeh, M. S. Alabed, and M. Guizani, "Energy efficient integration of renewable energy sources in the smart grid for demand side management," *IEEE Access*, vol. 6, pp. 77 077–77 096, 2018.

[6] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam, and S. M. Mazinani, "A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1495–1502, 2020.

[7] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of smart meter data analytics: Applications, methodologies, and challenges," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3125–3148, 2018.

[8] D. Alahakoon and X. Yu, "Smart electricity meter data intelligence for future energy systems: A survey," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 425–436, 2015.

[9] A. Chehri, I. Fofana, and X. Yang, "Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence," *Sustainability*, vol. 13, no. 6, p. 3196, 2021.

[10] Nist framework and roadmap for smart grid interoperability standards, release 1.0. [Online]. Available: https://www.nist.gov/system/files/documents/public_affairs/releases/smartgrid_interoperability_final.pdf

[11] L. Sattler and D. Pacella, "Quantum Key Distribution (QKD): Safeguarding for the Future," Online,https://www.comsoc.org/publications/ctn/quantum-key-distribution-qkd-safeguarding-future, [Accessed: Feb 2023].

[12] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.

[13] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212–219.

[14] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying grover's algorithm to aes: quantum resource estimates," in *Post-Quantum Cryptography*. Springer, 2016, pp. 29–43.

[15] R. Asif, "Post-quantum cryptosystems for internet-of-things: a survey on lattice-based algorithms," *IoT*, vol. 2, no. 1, pp. 71–91, 2021. [Online]. Available: https://www.mdpi.com/2624-831X/2/1/5

[16] X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, "Quantum security analysis of aes," *IACR Transactions on Symmetric Cryptology*, vol. 2019, no. 2, pp. 55–93, 2019.

[17] D. J. Bernstein and T. Lange, "Post-quantum cryptography—dealing with the fallout of physics success," Cryptology ePrint Archive, Paper 2017/314, 2017, https://eprint.iacr.org/2017/314. [Online]. Available: https://eprint.iacr.org/2017/314

[18] A. Shahidinejad and J. Abawajy, "An all-inclusive taxonomy and critical review of blockchain-assisted authentication and session key generation protocols for iot," *ACM Computing Surveys*, 2024. [Online]. Available: https://doi.org/10.1145/3645087

[19] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[20] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[21] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Reviews of Modern Physics*, vol. 92, no. 2, p. 025002, 2020.

[22] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Physical review letters*, vol. 108, no. 13, p. 130502, 2012.

[23] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical review letters*, vol. 108, no. 13, p. 130503, 2012.

[24] C. Wang, W. Y. Kon, H. J. Ng, and C. C.-W. Lim, "Experimental symmetric private information retrieval with measurement-device-independent quantum network," *Light: Science & Applications*, vol. 11, no. 1, p. 268, 2022.

[25] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *npj Quantum Information*, vol. 2, no. 1, pp. 1–9, 2016.

[26] D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ecc-based self-certified key distribution scheme for the smart grid," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 10, pp. 7996–8004, 2018.

[27] J. Srinivas, A. K. Das, X. Li, M. K. Khan, and M. Jo, "Designing anonymous signature-based authenticated key exchange scheme for internet of things-enabled smart grid systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 4425–4436, 2020.

[28] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1900–1910, 2018.

[29] F. Wu, L. Xu, X. Li, S. Kumari, M. Karuppiah, and M. S. Obaidat, "A lightweight and provably secure key agreement system for a smart grid with elliptic curve cryptography," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2830–2838, 2018.

[30] S. Garg, K. Kaur, G. Kaddoum, J. J. Rodrigues, and M. Guizani, "Secure and lightweight authentication scheme for smart metering infrastructure in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3548–3557, 2019.

[31] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3953–3962, 2018.

[32] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Generation Computer Systems*, vol. 81, pp. 557–565, 2018.

[33] D. Abbasinezhad-Mood and M. Nikooghadam, "Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications," *Future Generation Computer Systems*, vol. 84, pp. 47–57, 2018.

[34] D. Abbasinezhad-Mood and M. Nikooghadam, "Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended chebyshev chaotic maps," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4815–4828, 2018.

[35] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 237–249.

[36] J. Ahn, J. Chung, T. Kim, B. Ahn, and J. Choi, "An overview of quantum security for distributed energy resources," in *2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*. IEEE, 2021, pp. 1–7.

[37] Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec, and P. Zhang, "Quantum-secure microgrid," *IEEE Transactions on Power Systems*, vol. 36, no. 2, pp. 1250–1263, 2020.

[38] K. Prateek, S. Maity, and R. Amin, "An unconditionally secured privacy-preserving authentication scheme for smart metering infrastructure in smart grid," *IEEE Transactions on Network Science and Engineering*, 2022.

[39] Y. Li, P. Zhang, and R. Huang, "Lightweight quantum encryption for secure transmission of power data in smart grid," *IEEE Access*, vol. 7, pp. 36 285–36 293, 2019.

[40] J. Ahn, H.-Y. Kwon, B. Ahn, K. Park, T. Kim, M.-K. Lee, J. Kim, and J. Chung, "Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (pqc) and quantum key distribution (qkd)," *Energies*, vol. 15, no. 3, p. 714, 2022.

[41] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of modern physics*, vol. 81, no. 3, p. 1301, 2009.

[42] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Reviews of Modern Physics*, vol. 89, no. 1, p. 015004, 2017.

[43] Josh Schneider, Ian Smalley, "What is a qubit?" Online,https://www.ibm.com/topics/qubit#:~:text=A%20qubit%2C%20or%20quantum%20bit,to%20encode%20information%20in%20binary, [Accessed: Apr 2024].

[44] G. Samuels, D. Dutta, P. Mahon, and S. V. Nikam, "The importance of bell states in quantum computing," in *16th International Conference on Information Technology-New Generations (ITNG 2019)*. Springer, 2019, pp. 581–585.

[45] I. W. Primaatmaja, E. Lavie, K. T. Goh, C. Wang, and C. C. W. Lim, "Versatile security analysis of measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 99, no. 6, p. 062332, 2019.

[46] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," *Nature communications*, vol. 5, no. 1, p. 3732, 2014.

[47] A. Acín and L. Masanes, "Certified randomness in quantum physics," *Nature*, vol. 540, no. 7632, pp. 213–219, 2016.

[48] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan *et al.*, "Device-independent randomness expansion against quantum side information," *Nature Physics*, vol. 17, no. 4, pp. 448–451, 2021.

[49] C. Wang, I. W. Primaatmaja, H. J. Ng, J. Y. Haw, R. Ho, J. Zhang, G. Zhang, and C. Lim, "Provably-secure quantum randomness expansion with uncharacterised homodyne detection," *Nature Communications*, vol. 14, no. 1, p. 316, 2023.

[50] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

[51] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *International conference on the theory and applications of cryptographic techniques*. Springer, 2001, pp. 453–474.

[52] A. Shahidinejad and D. Abbasinezhad-Mood, "Ultra-lightweight and secure blockchain-assisted charging scheduling scheme for vehicular edge networks by utilization of nanopi neo," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 8, pp. 8116–8123, 2022.

[53] H. Ghaemi, D. Abbasinezhad-Mood, A. Ostad-Sharif, and Z. Alizadehsani, "Novel blockchain-assisted fault-tolerant roaming authentication protocol for mobility networks without home agent entanglement," *Journal of Network and Computer Applications*, p. 103843, 2024.

[54] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Public Key Cryptography-PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005. Proceedings 8*. Springer, 2005, pp. 65–84.

[55] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[56] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Phys. Rev. Lett.*, vol. 91, no. 5, p. 057901, 2003.

[57] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, Jun. 2005.

[58] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230503, Jun. 2005.

[59] Y. Wang, I. W. Primaatmaja, E. Lavie, A. Varvitsiotis, and C. C. W. Lim, "Characterising the correlations of prepare-and-measure quantum networks," *npj Quantum Inf.*, vol. 5, no. 1, p. 17, 2019.

Rohini Poolat Parameswarath received a Master of Technology degree in Software Engineering from the National University of Singapore, Singapore in 2009. She is a cyber security researcher at the Department of Electrical and Computer Engineering, National University of Singapore. Currently, she is pursuing a PhD with research focusing on protocols for security and privacy in vehicular environments. Before joining the National University of Singapore, she was part of the cyber security research team at the Singapore University of Technology and Design, Singapore. Before embarking on her career in cyber security research, she worked as a software engineer in multinational companies. She is passionate about finding solutions to the current challenges in the cybersecurity landscape. Her research interests include cyberattack detection, ways to prevent attacks, privacy, and cryptographic protocols in domains such as the Internet of Things (IoT), cyber-physical systems, and vehicular networks.

Chao Wang received his B.Sc. in Physics from Huazhong University of Science and Technology in 2013, followed by a Ph.D. in Physics from the University of Science and Technology of China in 2018. Currently, he serves as a Senior Research Fellow in the Department of Electrical and Computer Engineering at the National University of Singapore. His primary research interests include quantum communication, quantum cryptography, and quantum networks.

Biplab Sikdar is a Professor in the Department of Electrical and Computer Engineering at the National University of Singapore, where he also serves as the Head of the Department of Electrical and Computer Engineering. He received the B. Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He was an Assistant Professor from 2001-2007 and Associate Professor from 2007-2013 in the Department of Electrical, Computer, and Systems Engineering at Rensselaer Polytechnic Institute from 2001 to 2013. He is a recipient of the NSF CAREER award, the Tan Chin Tuan fellowship from NTU Singapore, the Japan Society for Promotion of Science fellowship, and the Leiv Eiriksson fellowship from the Research Council of Norway. His research interests include IoT and cyber-physical system security, network security, and network performance evaluation. Dr. Sikdar is a member of Eta Kappa Nu and Tau Beta Pi. He has served as an Associate Editor for the IEEE Transactions on Communications, IEEE Transactions on Mobile Computing, and IEEE Internet of Things Journal and is an IEEE COMSOC and VTS Distinguished Lecturer and ACM Distinguished Speaker.